OSPF and OSPFv3 Protocol

Feature history for OSPF and OSPFv3 protocol

Table 1: Feature History

Feature	Release Information	Description
OSPFv3 Support on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.2 Cisco vManage Release 20.3.1	Open Shortest Path First version 3 (OSPFv3) is an IPv4 and IPv6 link-state routing protocol that supports IPv6 and IPv4 unicast address families.
OSPFv3 IPSec Authentication	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	OSPFv3 authentication protects OSPFv3 routing payload with IPSec encryption and hashing. The solution is based on statically configured cryptographic keys that build on top of crypto map solutions. OSPFv3 is supported on service side and transport side.

OSPF and OSPFv3 protocol

OSPF

OSPF (Open Shortest Path First) is a widely used link-state routing protocol designed for Internet Protocol (IP) networks. As an Interior Gateway Protocol (IGP), it operates within a single autonomous system (AS). OSPF gathers link-state information from routers to construct a topology map of the network.

The Cisco Catalyst SD-WAN overlay network supports OSPF unicast routing protocols. You can configure these protocols on Cisco IOS XE Catalyst SD-WAN devices in any Virtual Routing and Forwarding (VRF) except for transport and management VRFs to provide reachability to networks at their local site Cisco IOS XE Catalyst SD-WAN devices can redistribute route information learned from OSPF into Overlay Management Protocol (OMP) so that OMP can better choose paths within the overlay network. When the devices at a local site do not connect directly to the WAN cloud but are one or more hops from the WAN and connect indirectly through a non-Cisco SD-WAN device, standard routing must be enabled on the DTLS connections of the devices so that they can reach the WAN cloud. OSPF can be the routing protocol.

The OSPF sessions run over a DTLS connection created on the loopback interface in VRF 0, the transport VRF responsible for carrying control traffic in the overlay network. The Cisco SD-WAN Validator learns about this DTLS connection via the loopback interface and conveys this information to theCisco SD-WAN Controller so that it can track the TLOC-related information. In VRF 0, you also configure the physical interface that connects the Cisco IOS XE Catalyst SD-WAN device to its neighbor—either the PE router in the MPLS case or the hub or next-hop router in the local site—but you do not establish a DTLS tunnel connection on that physical interface.

OSPFv3

OSPFv3 is an enhanced version of the OSPF routing protocol specifically designed for IPv6 networks. A significant change in OSPFv3 is the decoupling of IP addressing from the routing topology information. OSPFv3 is a routing protocol for IPv4 and IPv6 address families. It is a link-state protocol that makes its routing decisions based on the states of the links that connect source and destination machines. The state of a link is a description of that interface and its relationship to its neighboring networking devices. The interface information includes the IPv6 prefix of the interface, the network mask, the type of network it is connected to, the devices connected to that network, and more. This information is propagated in various type of link-state advertisements (LSAs).

Much of OSPFv3 is the same as in OSPF version 2. OSPFv3, which is described in RFC 5340, expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses.

For address family IPv6, OSPFv3 routes are referred to OSPF routes, and OSPFv3 internal routes (intra-area and inter-area) are implicitly advertised to OMP. OSPFv3 external routes (both AS-External and NSSA) can be explicitly advertised in OMP using the advertise OSPF external configuration. This is consistent with OSPF routes in address family IPv4 where OSPF internal routes are implicitly advertised in OMP. Similarly, OSPF external routes can be explicitly advertised to OMP using the advertise OSPF external configuration.

For address family IPv4, OSPFv3 routes are referred to as OSPFv3 routes and OSPFv3 internal routes are not implicitly advertised in OMP. All OSPFv3 IPv4 routes can be advertised in OMP using the advertise OSPFv3 configuration. OSPFv3 integration in controller mode is not supported.

OSPFv3 IPSec authentication

OSPFv3 IPSec authentication refers to a security mechanism used in IPv6 networks where Open Shortest Path First version 3 (OSPFv3) routing protocol packets are authenticated and optionally encrypted through the IP Security (IPSec) protocol. In order to ensure that OSPFv3 packets are not altered and re-sent to the device, OSPFv3 packets must be authenticated. OSPFv3 uses the IPSec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

Since OSPFv3 does not provide built-in authentication or encryption, IPSec is employed to ensure the integrity and confidentiality of OSPFv3 routing messages exchanged between routers. This approach helps prevent unauthorized devices from modifying or injecting routing information and protects against unauthorized packet capture and replay attacks, thereby enhancing the security of routing updates in enterprise or service provider IPv6 networks. To implement OSPFv3 IPSec authentication, you must configure IPSec security associations between participating routers, specifying appropriate authentication (such as HMAC with SHA or MD5).

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

Each interface has a secure socket state:

- NULL: Do not create a secure socket for the interface if authentication is configured for the area.
- DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition.
- GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec.
- UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec.
- CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED.
- UNCONFIGURED: Authentication is not configured on the interface.

OSPFv3 will not send or accept packets while in the DOWN state.

Restrictions for OSPF and OSPFv3 protocols

- The OSPF for IPv6 (OSPFv3) authentication with IPSec feature is not supported on the IP BASE license package. The Advanced Enterprise Services package license must be used.

- OSPFv3 encryption is not supported.
- The OSPFv3 configuration is supported only on interface-level using configuration groups. However, both interface-level and area-level configuration is supported using CLI add-on templates.

Prerequisites for OSPFv3 IPSec authentication

Configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3 to enable authentication.

Configure OSPF

To configure OSPF on a device using SD-WAN Manager templates:

Procedure

Step 1 Create an OSPF feature template to configure OSPF parameters. OSPF can be used for transport-side routing to enable communication between the Cisco IOS XE Catalyst SD-WAN devices when the router is not directly connected to the WAN cloud.

Step 2 Create a VPN feature template to configure VPN parameters for transport-side OSPF routing (in VPN 0). See the VPN help topic for more information.

Create OSPF template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 Click **Create Template**.

Step 4 From the **Create Template** drop-down list, choose **From Feature Template**.

Step 5 From the **Device Model** drop-down list, select the type of device for which you are creating the template. To create a template for VPN 0 or VPN 512:

a. Click **Transport & Management VPN** located directly beneath the **Description** field, or scroll to the **Transport & Management VPN** section.

b. Under **Additional VPN 0 Templates**, click **OSPF**.

c. From the **OSPF** drop-down list, click **Create Template**. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.

Step 6 To create a template for VPNs 1 through 511, and 513 through 65530:

a. Click **Service VPN** located directly beneath the **Description** field, or scroll to the **Service VPN** section.

b. Click the **Service VPN** drop-down list.

c. Under **Additional VPN Templates**, click **OSPF**.

d. From the **OSPF** drop-down list, click **Create Template**. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.

Step 7 In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and choose one of the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco SD-WAN device to a device template . When you click **Device Specific**, the **Enter Key** box opens. This box displays a key,which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco SD-WAN device to a device template. For more information, see *Create a Template Variables Spreadsheet*. To change the default key, type a new string and move the cursor out of the **Enter Key** box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Create basic OSPF

Procedure

To configure basic OSPF, select **Basic Configuration** and then configure the following parameters. All these parameters are optional.

Table 2:

Parameter Name	Description
Router ID	Enter the OSPF router ID in decimal four-part dotted notation. This is the unique 32-bit identifier associated with the OSPF router for Link-State Advertisements (LSAs) and adjacencies.
Distance for External Routes	Specify the OSPF route administration distance for routes learned from other domains. *Range:* 0 through 255 *Default:* 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. *Range:* 0 through 255 *Default:* 110
Distance for Intra-Area Routes	Specify the OSPF route administration distance for routes within an area. *Range:* 0 through 255 *Default:* 110

Redistribute routes into OSPF

To redistribute routes learned from other protocols into OSPF:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

Step 3 Click **Create Template**.

Step 4 From the **Create Template** drop-down list, choose **From Feature Template**.

Step 5 From the **Device Model** drop-down list, select the type of device for which you are creating the template. To create a template for VPN 0 or VPN 512:

a. Click **Transport & Management VPN** located directly beneath the **Description** field, or scroll to the **Transport & Management VPN** section.

b. Under **Additional VPN 0 Templates**, click **OSPF**.

c. From the **OSPF** drop-down list, click **Create Template**. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.

Step 6 To redistribute routes learned from other protocols into OSPF on Cisco SD-WAN devices, choose **Redistribute** > **Add New Redistribute** and configure the following parameters:

Table 3:

Parameter Name	Description
Protocol	Choose the protocol from which to redistribute routes into OSPF. Choose from BGP, Connected, NAT, OMP, EIGRP and Static.
Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

What to do next

To add another OSPF route redistribution policy, click the plus sign (+).

To remove an OSPF route redistribution policy from the template configuration, click **the trash icon** to the right of the entry.

To save the feature template, click **Save**.

Configure Interfaces in an OSPF area

Procedure

Step 1 To configure an OSPF area within a VPN on a Cisco IOS XE Catalyst SD-WAN device, choose **Area** > **Add New Area**. For OSPF to function, you must configure area 0.

Table 4:

Parameter Name	Description
Area Number	Enter the number of the OSPF area. *Range:* 32-bit number
Set the Area Type	Choose the type of OSPF area, Stub or NSSA.
No Summary	Click **On** to not inject OSPF summary routes into the area.
Translate	If you configured the area type as NSSA, choose when to allow Cisco IOS XE Catalyst SD-WAN devices that are ABRs (area border routers) to translate Type 7 LSAs to Type 5 LSAs: • **Always**—Router always acts as the translator for Type 7 LSAs. That is no other router, even if it is an ABR, can be the translator. If two ABRs are configured to always be the translator, only one of them actually ends up doing the translation. • **Candidate**—Router offers translation services, but does not insist on being the translator. • **Never**—Translate no Type 7 LSAs.

Step 2 Click **Add** to save the new area.

Step 3 To configure the properties of an interface in an OSPF area, choose **Add Interface**. In the **Add Interface** popup, configure the following parameters:

Table 5:

Parameter Name	Description
Interface Name	Enter the name of the interface, in the format **ge** *slot*/*port* or **loopback** *number*.
Hello Interval	Specify how often the router sends OSPF hello packets. *Range:* 1 through 65535 seconds *Default:* 10 seconds
Dead Interval	Specify how often the Cisco IOS XE Catalyst SD-WAN device must receive an OSPF hello packet from its neighbor. If no packet is received, the Cisco IOS XE Catalyst SD-WAN device assumes that the neighbor is down. *Range:* 1 through 65535 seconds *Default:* 40 seconds (4 times the default hello interval)
LSA Retransmission Interval	Specify how often the OSPF protocol retransmits LSAs to its neighbors. *Range:* 1 through 65535 seconds *Default:* 5 seconds
Interface Cost	Specify the cost of the OSPF interface. *Range:* 1 through 65535

Step 4 To configure advanced options for an interface in an OSPF area, in the **Add Interface** popup, click **Advanced Options** and configure the following parameters:

Table 6:

Parameter Name	Description
Designated Router Priority	Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR. *Range:* 0 through 255 *Default:* 1
OSPF Network Type	Choose the OSPF network type to which the interface is to connect: • Broadcast network—WAN or similar network. • Point-to-point network—Interface connects to a single remote OSPF router. • Non-broadcast—Point-to-multipoint. *Default:* Broadcast
Passive Interface	Click **On** or **Off** to specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol. *Default:* Off
Authentication	Specify the authentication and authentication key on the interface to allow OSPF to exchange routing update information securely.

Parameter Name	Description
• **Authentication Type**	Choose the authentication type: • Simple authentication—Password is sent in clear text. • Message-digest authentication—MD5 algorithm generates the password.
• **Authentication Key**	Enter the authentication key. Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. The key can be 1 to 32 characters.
• **Message Digest**	Specify the key ID and authentication key if you are using message digest (MD5).
• **Message Digest Key ID**	Enter the key ID for message digest (MD5 authentication). It can be 1 to 32 characters.
• **Message Digest Key**	Enter the MD5 authentication key in clear text or as an AES-encrypted key. It can be from 1 to 255 characters.

Step 5 Click **Save** to save the interface configuration.

Configure an interface range for summary LSAs

Procedure

Step 1 To configure the properties of an interface in an OSPF area, choose **Area** > **Add New Area** > **Add Range**. In the **Area Range** popup, click **Add Area Range**, and configure the following parameters:

Table 7:

Parameter Name	Description
Address	Enter the IP address and subnet mask, in the format *prefix*/*length* for the IP addresses to be consolidated and advertised.
Cost	Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. *Range:* 0 through 16777215
No Advertise	Click **On** to not advertise the Type 3 summary LSAs or **Off** to advertise them.

Step 2 Click **Save** to save the area range.

Configure other OSPF properties

Procedure

Step 1 To configure other OSPF properties, click **Advanced** and configure the following properties:

Table 8:

Parameter Name	Description
Reference Bandwidth	Specify the reference bandwidth for the OSPF auto-cost calculation for the interface. *Range:* 1 through 4294967 Mbps *Default:* 100 Mbps
RFC 1538 Compatible	By default, the OSPF calculation is done per RFC 1583. Click **Off** to calculate the cost of summary routes based on RFC 2328.
Originate	Click **On** to generate a default external route into an OSPF routing domain: • Always—Click **On** to always advertise the default route in an OSPF routing domain. • Default metric—Set the metric used to generate the default route. *Range:* 0 through 16777214 *Default:* 10 • Metric type—Select to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
SPF Calculation Delay	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. *Range*: 0 through 600000 milliseconds (60 seconds) *Default*: 200 milliseconds
Initial Hold Time	Specify the amount of time between consecutive SPF calculations. *Range*: 0 through 600000 milliseconds (60 seconds) *Default*: 1000 milliseconds
Maximum Hold Time	Specify the longest time between consecutive SPF calculations. *Range*: 0 through 600000 *Default*: 10000 milliseconds (60 seconds)
Policy Name	Enter the name of a localized control policy to apply to routes coming from OSPF neighbors.

Step 2 Click **Save** to save the feature template.

Configure OSPFv3 IPSec authentication

Once you have configured OSPFv3 and decided on your authentication, you must define the security policy on each of the devices within the group. The security policy consists of the combination of the key and the SPI. To define a security policy, you must define an SPI and a key.

You can configure an authentication or encryption policy either on an interface or for an OSPFv3 area. When you configure for an area, the security policy is applied to all of the interfaces in the area. For higher security, use a different policy on each interface.

You can configure authentication on virtual links.

- Defining Authentication on an Interface
- Defining Authentication in an OSPFv3 Area

Configure OSPFv3 IPSec authentication at an interface-level using CLI

Before you begin

Follow these steps to configure OSPFv3 IPSec authentication at an interface-level using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# config-transaction
```

Step 2 In the configuration mode, configure an interface type such as, Gigabit Ethernet.

Specifies an interface type and number, and places the device in interface configuration mode.

Example:

```
Device(config)# interface GigabitEthernet3
```

Step 3 Configure OSPFv3 authentication on the interface.

Specifies the authentication type for an interface.

Example:

```
Device(config-if)# ospfv3 authentication ipsec spi 256 sha1 0 09876543210987654321098765432109876543210987654321
```

Configure OSPFv3 IPSec authentication at an area-level using CLI

Before you begin

Follow these steps to configure OSPFv3 IPSec authentication at an area-level.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# config-transaction
```

Step 2 Enable OSPFv3 router configuration mode.

Example:

```
Device(config)# router ospfv3 <process-id>
```

Step 3 Configure OSPFv3 authentication on the interface.

Enables authentication in an OSPFv3 area.

Example:

```
Device(config-rtr)# area <area-id> authentication ipsec spi <spi> authentication-algorithm
```

```
Device(config)# router ospfv3 <process-id>
Device(config-rtr)# area <> authentication ipsec spi <> [md5/sha1] <>
interface GigabitEthernetY/Y
ospfv3 <> [ipv4/ipv6] area <>
```

Configure OSPF using CLI

To set up routing on the Cisco IOS XE Catalyst SD-WAN device, you provision VRFs if segmentation is required. Within each VRF, you configure the interfaces that participate in that VRF and the routing protocols that operate in that VRF.

When configuring OSPF from the CLI, ensure that the OSPF process id (PID) and the VRF ID match for OMP redistribution of OSPF to work for the specified VRF. The process ID is the ID of the OSPF process to which the interface belongs. The process ID is local to the router and is used as an identifier of the local OSPF process.

Here is an example of configuring service-side OSPF on a Cisco IOS XE Catalyst SD-WAN device.

```
config-transaction
 router ospf 1 vrf1
  auto-cost reference-bandwidth 100
  max-metric router-lsa
  timers throttle spf 200 1000 10000
  router-id 172.16.255.15
  default-information originate
  distance ospf external 110
  distance ospf inter-area110
  distance ospf intra-area110
  distredistribute connected subnets route-map route_map
  exit
 interface GigabitEthernet0/0/1
  no shutdown
  arp timeout 1200
  vrf forwarding 1
```

```
 ip address 10.1.100.14 255.255.255.0
 ip redirects
 ip mtu 1500
 ip ospf 1 area 0
 ip ospf network broadcast
 mtu 1500
 negotiation auto
 exit
```

Configuration examples for IPv6 OSPFv3 IPSec authentication

You can configure OSPFv3 IPSec authentication on an interface or in an area.

Note Interface-level authentication takes priority over area-level authentication

Configuring IPv6 OSPFv3 authentication on an interface

This example shows how to define authentication on Ethernet interface 0/0:

```
interface Ethernet0/0
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv6 dead-interval 40
 ospfv3 1 ipv6 hello-interval 10
 ospfv3 1 ipv6 retransmit-interval 5
 ospfv3 authentication ipsec spi 256 sha1 0 09876543210987654321098765432109876543210
```

Configuring IPv6 OSPFv3 authentication in an area

This example shows how to define authentication on OSPFv3 area 0:

```
router ospfv3 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 256 sha1 0 09876543210987654321098765432109876543210
```